

INSTALACIÓN Y CONFIGURACIÓN DE GNU/LINUX ZENTYAL SERVER E IMPLEMENTACIÓN DE SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA IT

Lady Lorena Ortiz Castillo
e-mail: llortizc@unadvirtual.edu.co
Sindy Carolina Diaz Aldana
e-mail: scdiazal@unadvirtual.edu.co
William Fernando López Jurado
e-mail: wflopezj@unadvirtual.edu.co
Jeffer Ricardo Bernal Góngora
e-mail: jrbernalg@unadvirtual.edu.co
Jhulian Javier Celis Gómez
e-mail: jjcelisg@unadvirtual.edu.co

RESUMEN: En este documento se describe en detalle la instalación y configuración de GNU/Linux Zentyal Server 5.0 y se realizan las respectivas pruebas realizando conexión hacia un equipo con GNU/Linux Debian 10. Se implementan los servicios DHCP Server, DNS Server y Controlador de Dominio, implementación y configuración de Proxy no transparente, configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas, configuración del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras y creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo.

PALABRAS CLAVE: Zentia, Debian, DHCP, DNS, Dominio, Firewall, VPN.

1 INTRODUCCIÓN

Para esta última entrega se instaló Zentyal Server a través de Virtual Box, esta es una versión gratuita de código abierto que nos ofrece varios servicios como lo son DHCP, DNS, Firewall, VPN, Mail Server entre otros. Este S.O es usado principalmente en pequeñas y medianas empresas ya que ofrece servicios especiales que normalmente solo se utilizan en infraestructuras de TI a gran escala. Es muy fácil de instalar y configurar, al instalar el SO Zentyal inicia un escritorio con una configuración mínima sobre la cual se desarrolló cada temática acorde a lo solicitado en la guía para el paso 8.

Para aumentar la seguridad de la red, Zentyal ofrece varios servicios de seguridad, como un filtro para contenido Web y un módulo antivirus. Para integrar a la perfección una máquina (PC) de Windows en una infraestructura existente, por ejemplo, la distribución implementa un servidor Samba. Establece un Dominio para clientes de Windows y permite el intercambio de datos sin problemas entre varios entornos del sistema. Por último, pero no menos importante, Zentyal viene con un módulo de copia de seguridad que facilita las copias de seguridad de datos.

2 INSTALACIÓN DE GNU/LINUX ZENTYAL SERVER 5.0

2.1 Requisitos

El servidor Zentyal puede funcionar sin ningún problema con 2 Gb de RAM, 8 GB de Disco Duro y un procesador de doble núcleo. Además, tener en cuenta la instalación de dos adaptadores de red para la red externa WAN y la red Interna LAN.

2.2 URL de descarga

Se descarga Zentyal Server 5.0 desde <http://download.zentyal.com/zentyal-5.0.1-development-amd64.iso>. Este será el archivo .ISO que contiene la imagen para la instalación de Zentyal Server.

2.3 Proceso de Instalación

1. Se inicia con la instalación de Zentyal Server 5.0

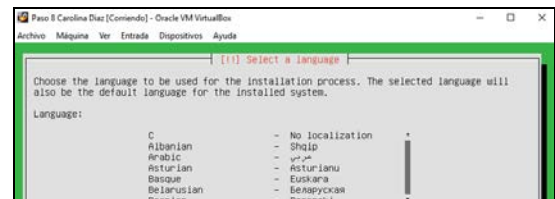


Fig. 1, Interfaz inicial para selección de idioma.

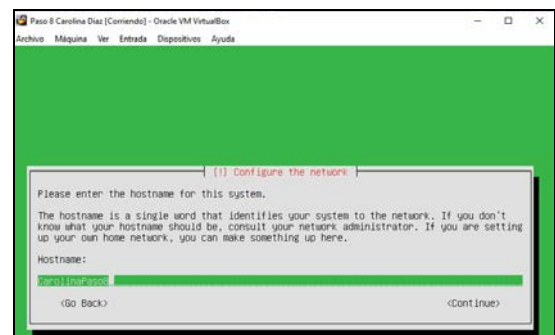


Fig. 2, Se nombra la máquina.

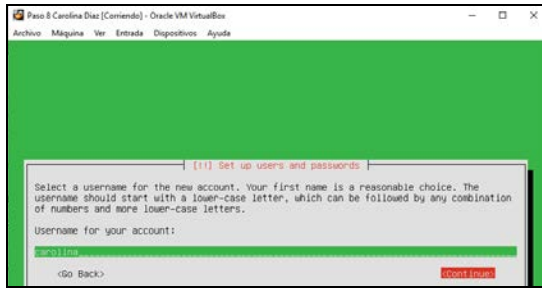


Fig. 3, Se asigna Contraseña de acceso

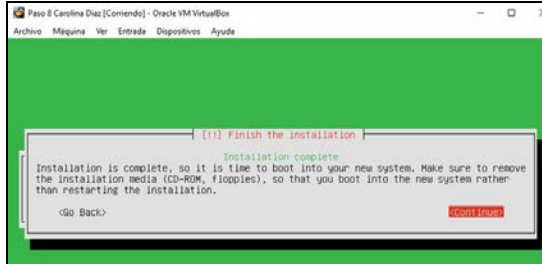


Fig. 4, Instalación Completada.

- Una vez finalizada la instalación reiniciar el sistema.

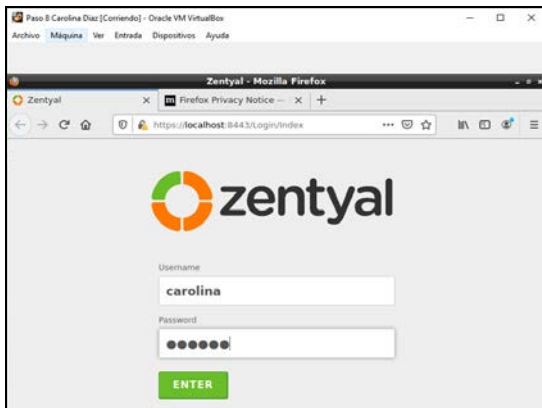


Fig. 5, Acceso a Zentyal.

3 CONFIGURACIÓN DE SERVICIOS

3.1 Temática 1 DHCP Server, DNS Server y Controlador de Dominio.

Solución Planteada:

En la sección de paquetes se activa el DNS Server, DHCP Server y el Controlador de Dominios.



Fig. 6, Seleccionar los servicios a instalar en el servidor.

- Se le asigna una IP estática al Servidor en la interfaz interna de la red.



Fig. 7, Configuración de Red.

- Se asigna un nombre para el controlador de Dominio, Zentyal.Local



FIG. 8, Se nombra del Dominio.

- Instalación ha finalizado correctamente.

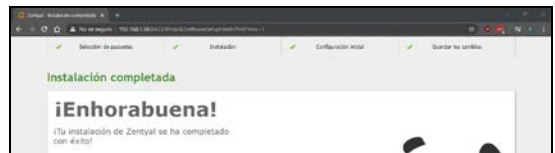


Fig. 9, Configuración completada.

- Se visualiza el tablero de Administración del servidor Zentyal.

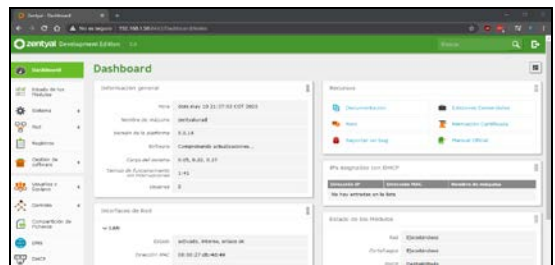


Fig. 10, Dashboard Zentyal.

- Configurar DNS para el Servidor Zentyal, esto permite la salida a internet de los equipos que se autentican en el Dominio.



Fig. 11, Configuración DNS.

8. Se valida que este habilitado el controlador de Dominio Zentyal. Local.

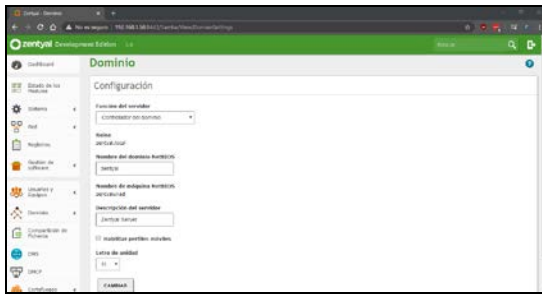


Fig. 12, Controlador de Dominio.

9. Se pueden agregar Grupos desde el controlador de dominio.

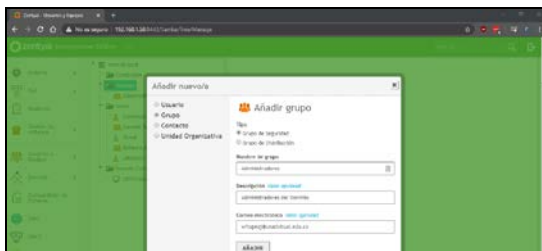


Fig. 13, Creación de grupos.

10. Desde la raíz del controlador de dominio se crea una unidad organizativa Tecnología.

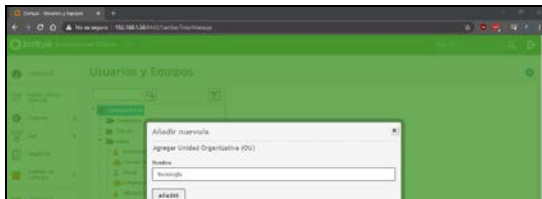


Fig. 14, Creación de unidad Organizativa.

11. En la nueva unidad organizativa se crea un usuario administrador **wflopezj**.

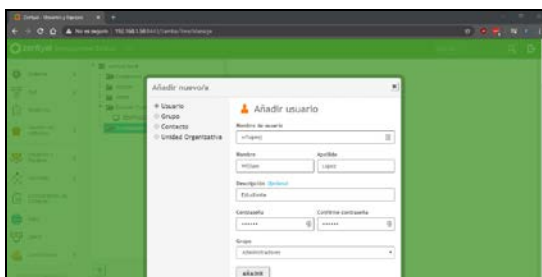


Fig. 15, Gestión de usuarios y Equipos

Se configura un rango de IPs. Éstas serán las que el Servidor DHCP asignará automáticamente.

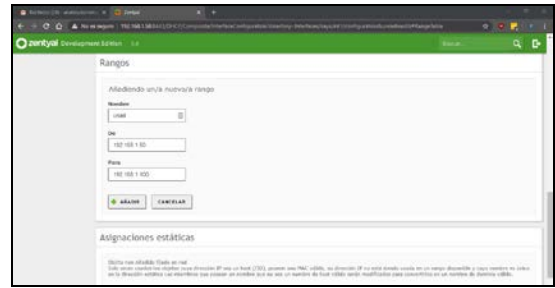


Fig. 16, DHCP Server

12. Se establece un rango de direcciones IP que se asignarán a los equipos que se unan al dominio.



Fig. 17, Rango de IPs.

13. Se puede configurar un tiempo de asignación de IP para cada equipo en la red.

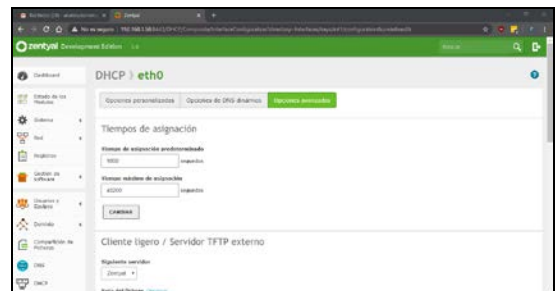


Fig. 18, Tiempos de Asignación

14. Se ingresa al archivo **resolv.conf** del equipo cliente que se ingresó como servidor DNS, la IP del servidor Zentyal se relaciona para que pueda ser unido al dominio.

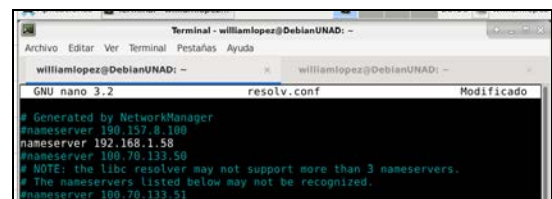
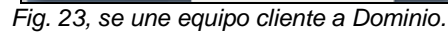
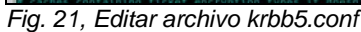


Fig. 19, DNS servidor Zentyal

15. Instalar los paquetes necesarios en el cliente de Linux:
sudo apt-get install sssd heimdal-clients msktutil



19. Se verifica que el equipo **DEBIANUNAD** se ha unido al dominio correctamente.



- 

Development Edition

5.0

Dashboard

Estado de los Módulos

Sistema

Red

Registros

Gestión de software

Usuarios y Equipos

Dominio

Usuarios y Equipos

zentyal.local

Computers

DEBIANUNAD

Groups

Administradores

diplomado

Users

Domain Admins

Guest

Schema Admins

Administrator

Domain Controllers

ZENTYALUNAD

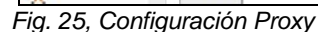
Fig. 24, Registro de equipo cliente en el Dominio.



- | | | | |
|---------------------------|----|-------|----|
| 3.2 Temática transparente | 2: | Proxy | no |
|---------------------------|----|-------|----|

Producto esperado: Implementación y configuración detallada del control del acceso de una estación GNU/Linux Debian 10 a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 830.

20. Se ingresa módulo proxy configuraciones generales y se valida la siguiente configuración



21. Validar que el módulo de proxy se encuentre habilitado

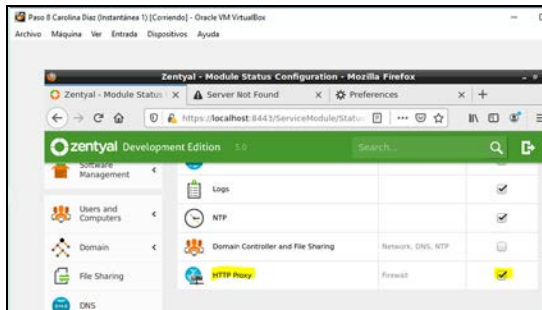


Fig. 26, Activación modulo HTTP Proxy

22. Se debe ingresar a la configuración del proxy desde el navegador.

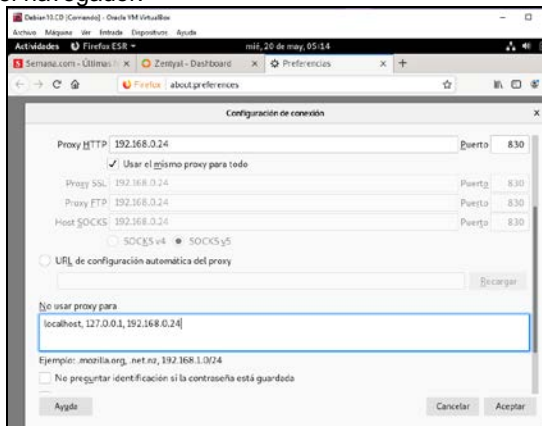


Fig. 27, Proxy navegador Debian 10

23. Se prueba que el equipo Debian tenga acceso a internet.



Fig. 28, Prueba de navegación Debian 10

24. Se bloquea la página semana.com, para esto ingresar a HTTP Proxy/Filter Profiles.

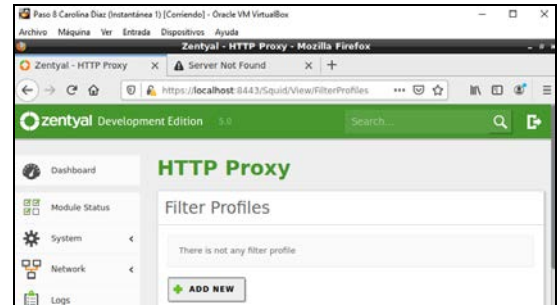


Fig. 29, Panel configuración Proxy.

25. Seleccionar add new y creamos el filtro

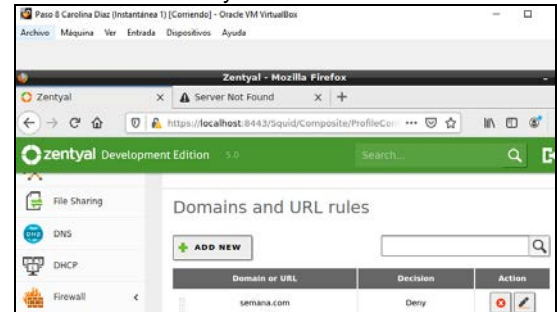


Fig. 30, Creación filtros Proxy.

26. Ingresar a la configuración, opción de Dominios y restringir el acceso a la página mencionada.

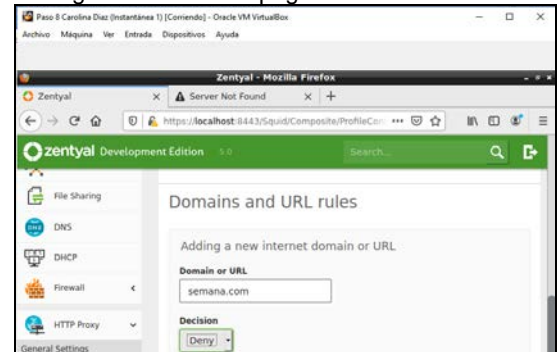


Fig. 31, Creación filtros Proxy.

27. Guardar cambios.

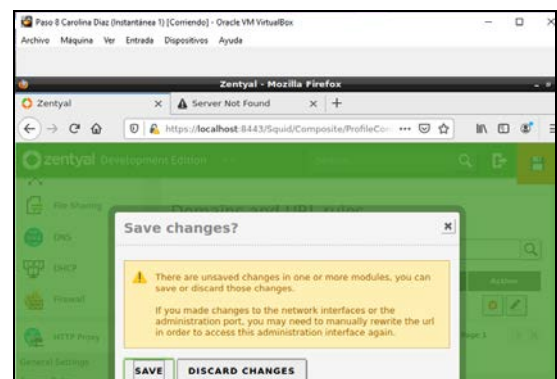


Fig. 32, Creación filtros Proxy.

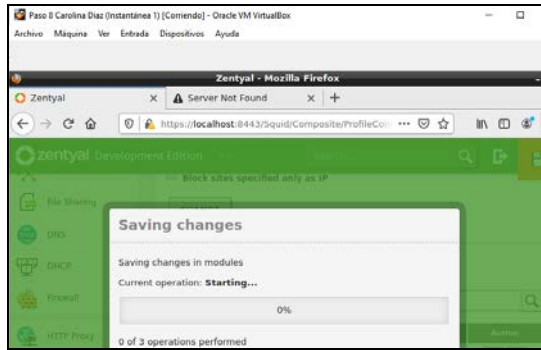


Fig. 33, Creación filtros Proxy.

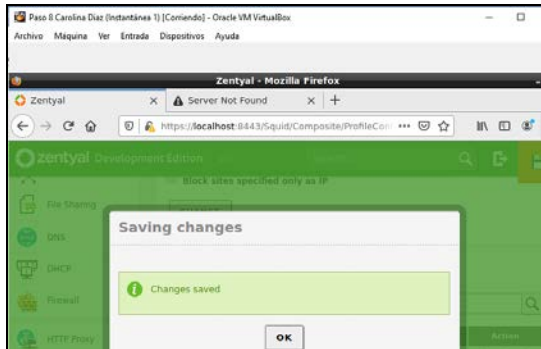


Fig. 34, Creación filtros Proxy.

28. Se ingresa nuevamente a la página semana.com desde el equipo Debian y se valida la restricción para acceder debido a la configuración de proxy.

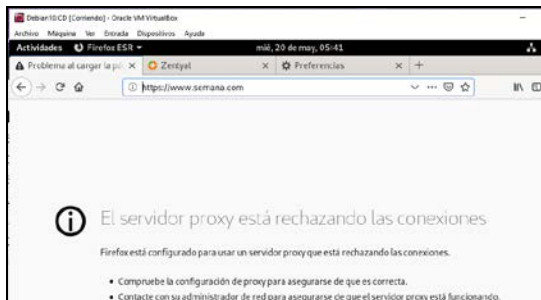


Fig. 35, Validación filtro Proxy.

29. Comprobar la conexión para las otras páginas que no tiene restricción y para el servidor Zentyal.

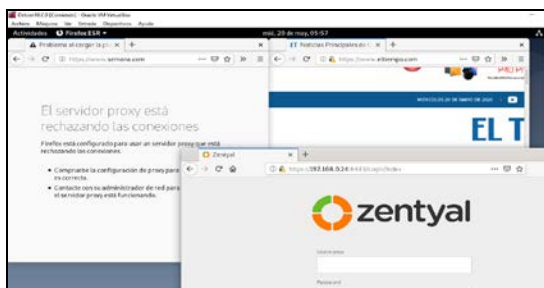


Fig. 36, Navegador Debian 10.

3.3 Temática 3: Cortafuegos

Producto esperado: Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Debian 10.

30. Seleccionar los paquetes necesarios para desarrollar el ejercicio: Firewall.

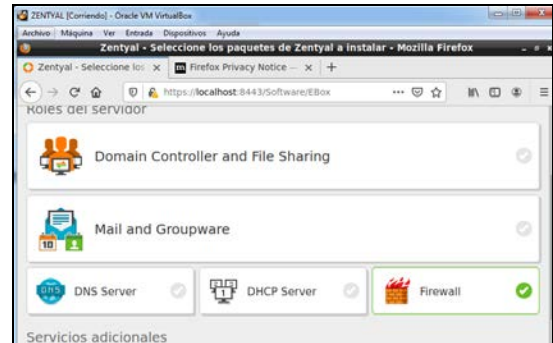


Fig. 37, Elección de Firewall

31. Se instalan

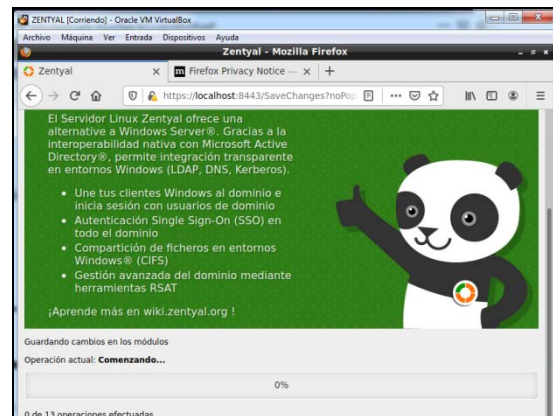


Fig. 38, Proceso de instalación

32. Se configura la interfaz de red.

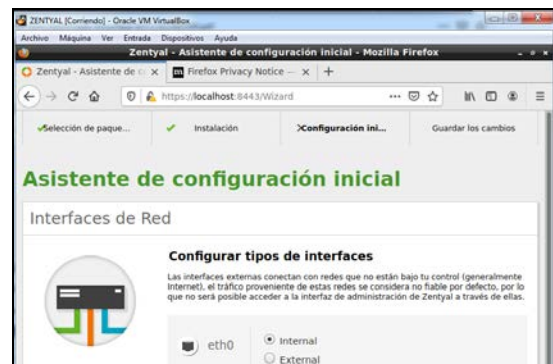


Fig. 39, Configuración interfaz

33. Seleccionar DHCP.

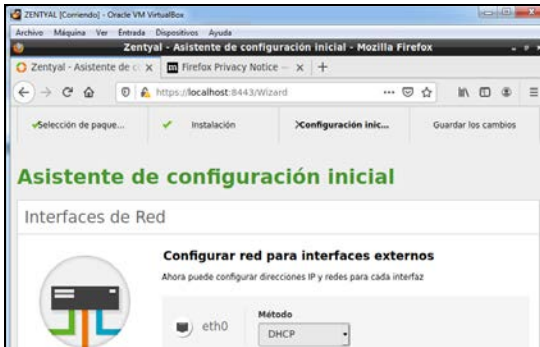


Fig. 40, Selección DHCP

34. Ingresar a dashboard-cortafuegos

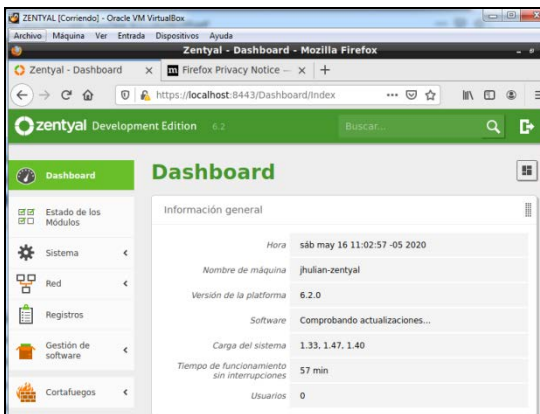


Fig. 41, Dashboard

35. Finalmente, para realizar los bloqueos a los sitios web es necesario conocer su dirección IP para generar el bloqueo de este. Esto se puede saber realizando un ping al sitio web que se quiera bloquear o también se puede generar por la palabra. Para realizar los bloqueos se ingresa a filtrado de paquetes.

36. Se configura una regla.



Fig. 42, Tráfico saliente

37. Debe hacerse en el filtrado para el tráfico saliente de Zentyal.

38. Se crea la regla.

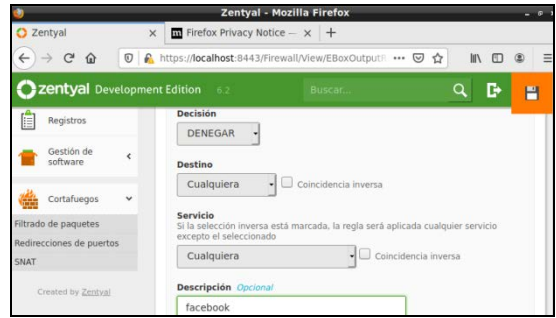


Fig. 43, Regla

39. Verificar la regla creada.



Fig. 44, Reglar aplicada

40. Guardar cambios.



Fig. 45, Guardar cambios

41. Se verifica que la regla y el bloqueo funcionó.



Fig. 46, Consulta

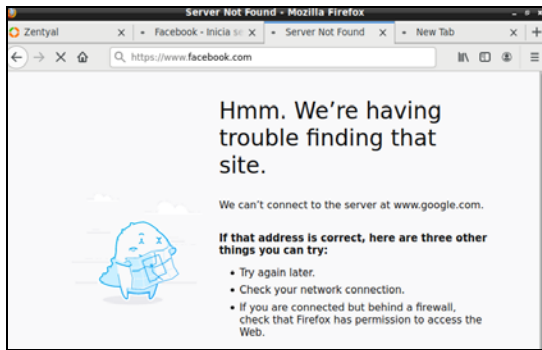


Fig. 47, Bloqueo efectivo

42. Se evidencia el filtrado y bloqueo de la página con la regla.

3.4 Temática 4: File Server

Producto esperado: Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Debian 10 a través del controlador de dominio LDAP a los servicios de carpetas compartidas.

43. Teniendo instalada Zentyal en la máquina virtual se continua con instalación del paquete de red. Luego de configurar la red y dominio, se continua con las demás instalaciones de paquete y se procede a crear los usuarios y grupos.

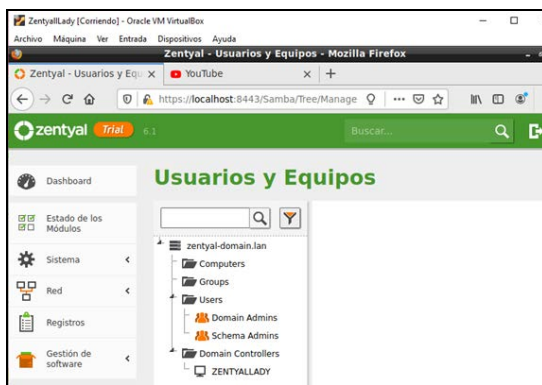


Fig. 48, Creación usuarios y grupos.

44. Se configura el control de acceso del o los usuarios, donde se asigna accesos y permisos de lectura y escritura.

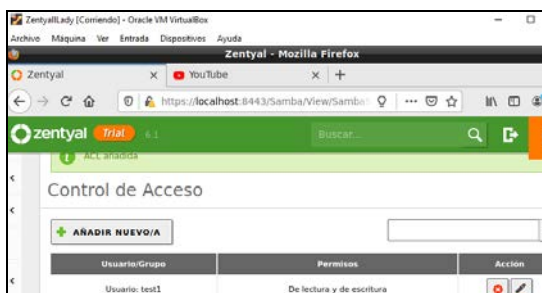


Fig. 49, Control de acceso

45. Ya teniendo el usuario, se habilita el servicio de directorio Samba (LDAP) para compartir los ficheros al servidor



Fig. 50, Configuración PAM.

46. Se accede al módulo de compartición de ficheros, agregando así recursos donde se ingresa por Desktop GNU/Linux.

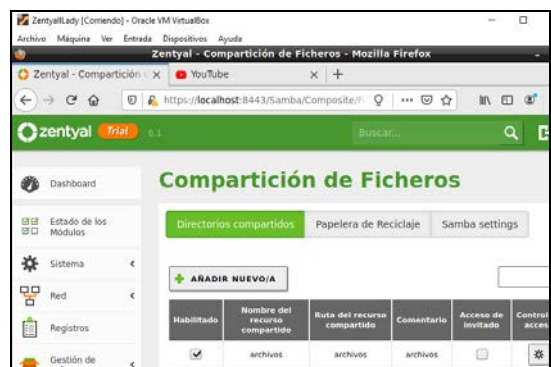


Fig. 51, Compartición de archivos.

47. Se configura el rango DHCP, donde se genera una interfaz de acceso en el Desktop y enseguida carga la lista de interfaces donde se consume el servicio.

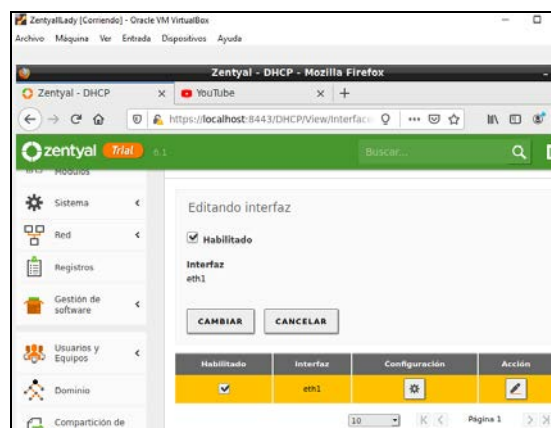


Fig. 52, Editar interfaz.

48. Antes de habilitar la interfaz solicita habilitar el módulo DHCP, se selecciona y se guarda se

ingresa al Dashboard para visualizar las IPs asignadas con DHCP.

49.

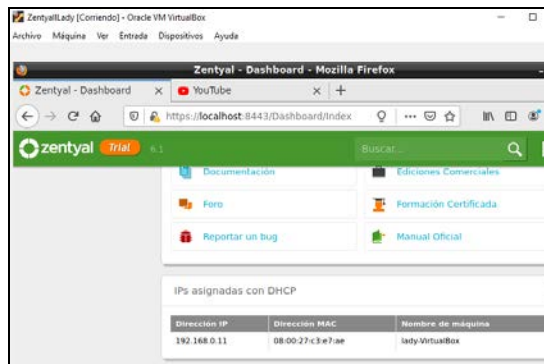


Fig. 53, IPs asignadas.

50. Para tener control y acceso al servidor por usuario y dominio es necesario instalar Active Directory Membership (likewise-open, libglade2 y likewise-open-gui) pero antes de iniciar el GUI revisarla la configuración del archivo resolv.conf.

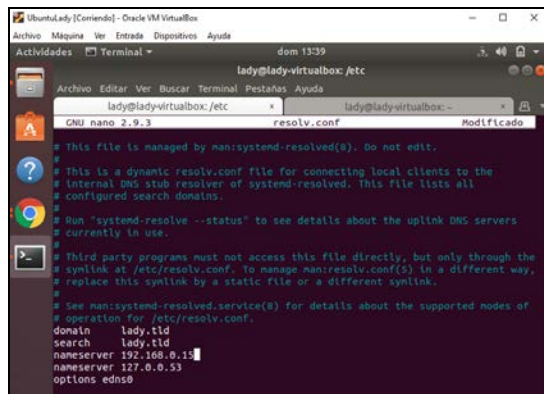


Fig. 54, Edición archivo.

51. Ejecutar el siguiente comando para acceder al entorno y realizar la configuración de conexión: (sudo domainjoin-gui) y agregar el Dominio de Zentyal.

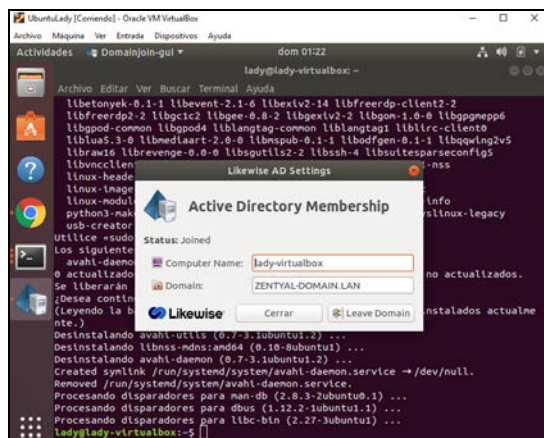


Fig. 55, Interfaz Active Directory Membership.

52. Se cargará la confirmación del acceso.

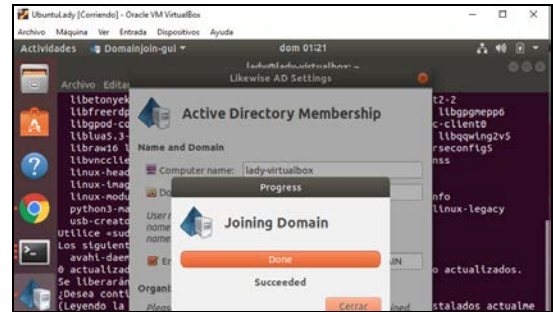


Fig. 56, Conexión satisfactoria.

53. Verificar el acceso debido que en el servidor de Zentyal se cargará en usuarios y equipos de la carpeta Computarse el nombre del equipo conectado.

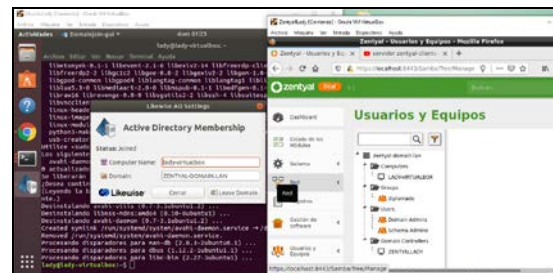


Fig. 57, Acceso servidor.

54. Cerrar sesión y acceder con el usuario configurado para visualizar las carpetas compartidas a ese usuario. Se conecta vía Samba, con la acción smb://{dominio Zentyal}

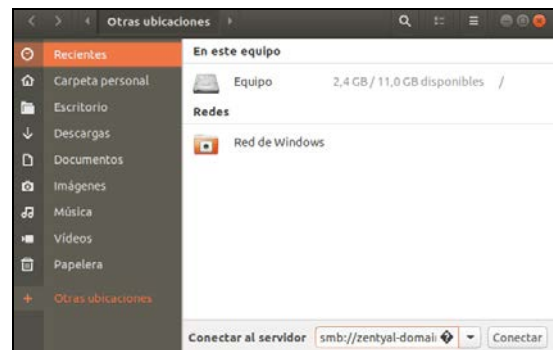


Fig. 58, Ingreso Samba.

55. Al acceder cargará el acceso de la carpeta creada en pasos anteriores.

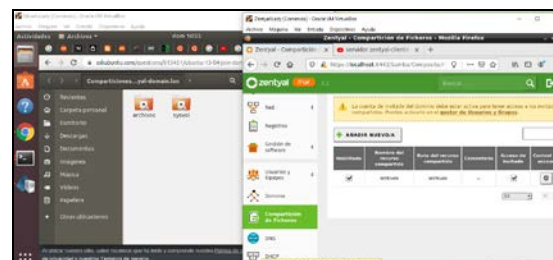


Fig. 59, Carpeta compartida.

56. Al tener el usuario permisos de lectura y escritura podrá agregar archivos y editarlos.

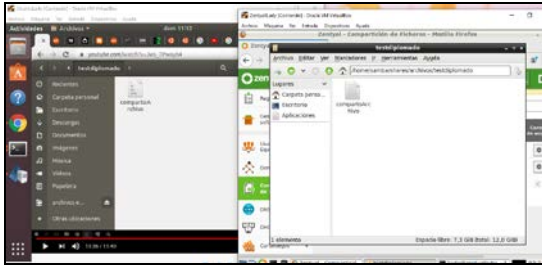


Fig. 60, Verificación de archivos.

57. Abrir consola y agregar el Cups de conexión para realizar la configuración de impresión.

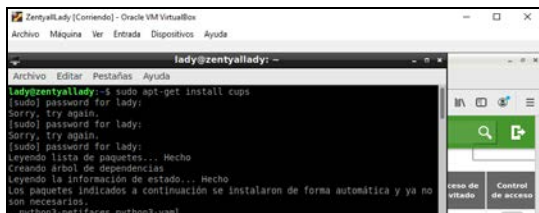


Fig. 61, Instalación Cups.

58. Acceder al dominio junto con el puerto 631 (específico para la configuración de impresión)

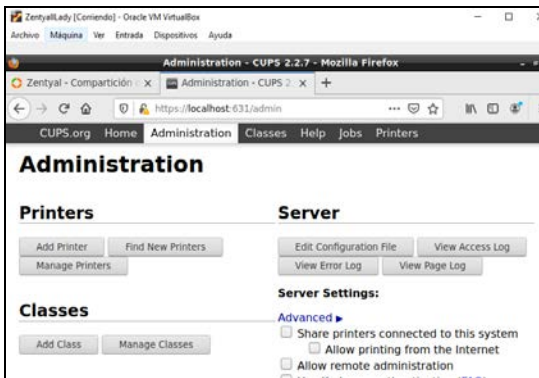


Fig. 62, Ingreso al Cups de configuración.

59. Seleccionar 'Add Printer' y agregar las credenciales de acceso.

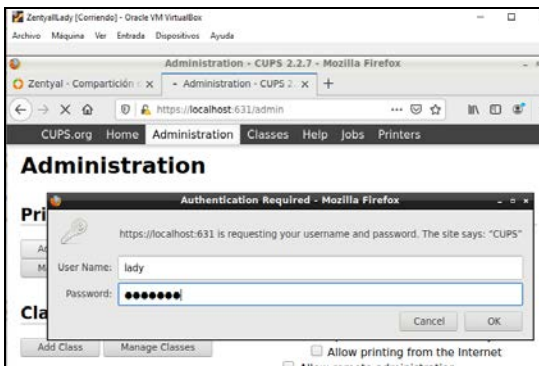


Fig. 63, credenciales de edición.

60. Seleccionar la opción de conexión

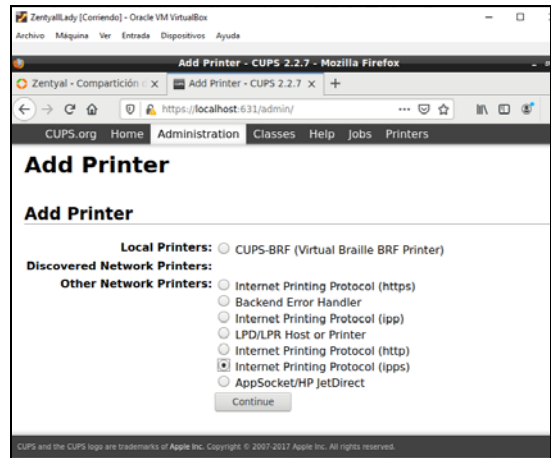


Fig. 64, Tipo de conexión.

61. Seleccionar la URL de conexión.

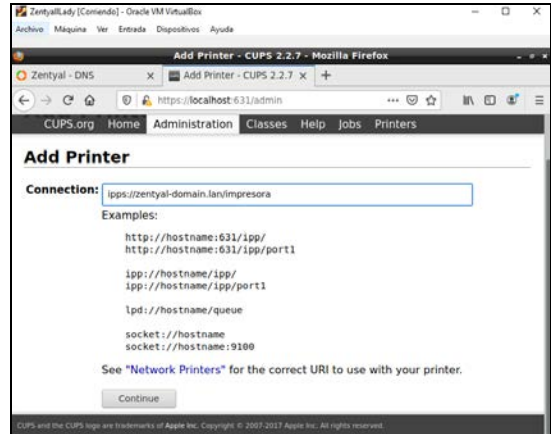


Fig. 65, Agregar URL de conexión.

62. Agregar nombre y ubicación de la carpeta, seleccionar 'Share this printer' para compartirla y acceder.

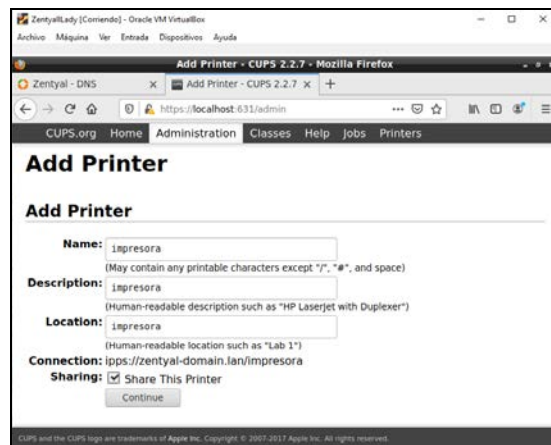


Fig. 66, Nombre y datos de localización.

63. Seleccionar el tipo de impresora

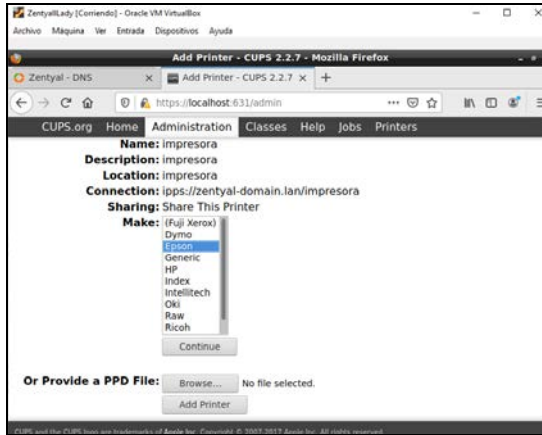


Fig. 67, Tipo de impresora.

64. Se ajusta tamaño y resolución de la impresora, carga mensaje exitoso de las opciones y/o configuración de la impresora. Finalmente acceder al Desktop de Linux, cargará la impresora CUPS configurada.

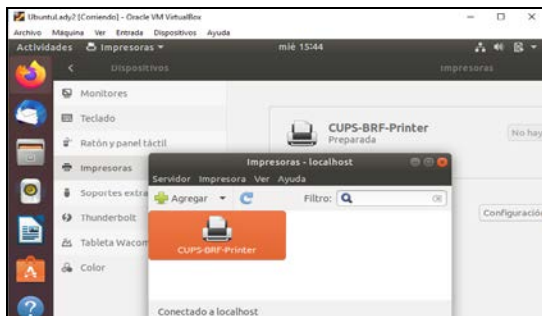


Fig. 68, Conexión impresora.

3.5 Temática 5: VPN

Producto esperado: Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Debian 10. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

Al tener Zentyal instalado correctamente se asigna una IP fija en este caso será 192.268.0.20, se ingresa a la opción red y en interfaces configura la puerta de enlace.



Fig. 69, Agregar ip fija al servidor

65. Se procede con la configuración de la VPN, ir a estados de módulos y validar la opción VPN.

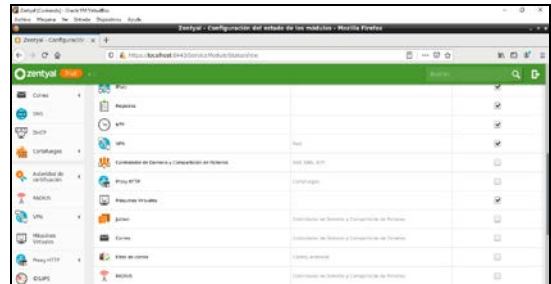


Fig. 70, Estados de modulo

66. Ahora en módulos buscar VPN - servidor – módulo de autoridad de certificados.

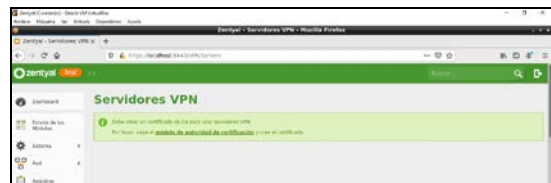


Fig. 71, Servidores VPN

67. Llenar los campos solicitados.



Fig. 72, Creación de certificado de conexión

68. Ingresar a la opción VPN-servidor y colocar un nombre para el servidor VPN.



Fig. 73, Generando nombre de servidor VPN

69. En la opción configuración, añadir el rango de IPs.



Fig. 74, Se agrega el rango de IPs locales

70. Se ingresa de nuevo en VPN-servidor y descargar paquete de configuración de cliente, crea un certificado
71. Generar un nombre, para el presente caso será VPN-Cliente

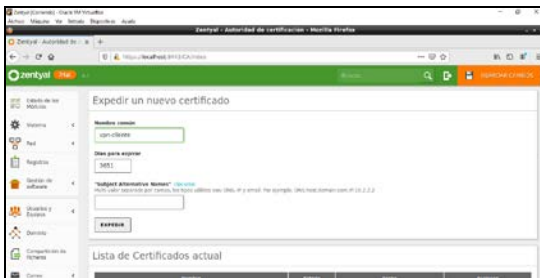


Fig. 75, Se expide certificado de conexión

72. Finalmente descargar la configuración, para Linux, colocar la IP del servidor 192.168.0.20



Fig. 76, Descarga de certificado cliente

73. Descomprimir el paquete descargado, ubicar por consola la carpeta de descargas y utilizar tar -xzf.



Fig. 77, Desempaquetar certificado descargado

74. Se valida la respectiva conexión openvpn vpn.jeffbernal.com.client.conf

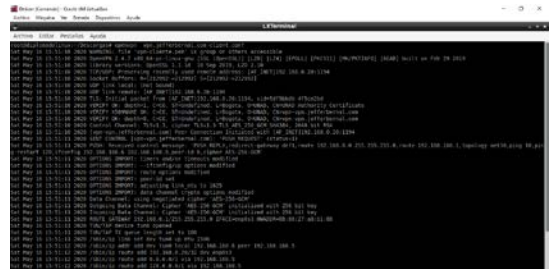


Fig. 78, Ejecutar certificado, Conexión exitosa

75. También validar pruebas de conexión en la maquina base con Windows 10, descargar el paquete para el S.O, descomprimir.

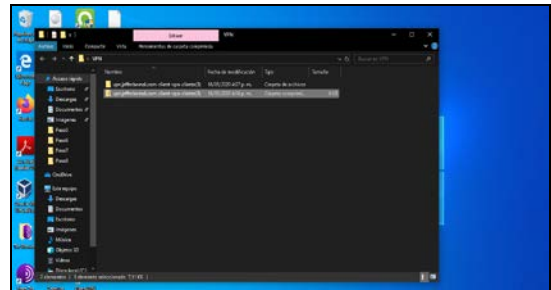


Fig. 79, Descomprimir certificado Windows

76. Abrir el cliente Openvpn y agregar el archivo descomprimido para la respectiva conexión

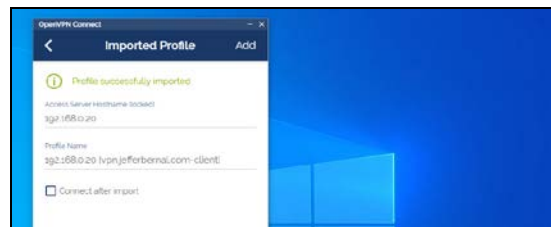


Fig. 80, Cargar certificado

77. Habilitar el botón de conexión y listo.

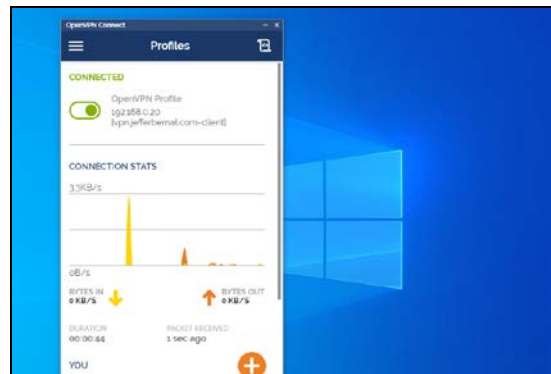


Fig. 81, Conexión exitosa

4 CONCLUSIONES

Durante nuestra experiencia con Zentyal nos ofreció un amplio conocimiento en el servidor, donde manejamos y exploramos todas las configuraciones de dominio (DNS), cortafuegos (Firewall), extensiones seguras en la red (VPN), manejo de impresora (Print Server- Cups), controles de acceso (Proxy).

Zentyal maneja un entorno grafico muy intuitivo y fácil de manejar y/o explorar, por medio de este logramos elaborar las temáticas de la forma más completa y entendible.

Elaboración apropiada en las configuraciones ya sea por medio de comandos o en el entorno gráfico que Zentyal nos ofrece.

5 REFERENCIAS

1. Celaya, L. A. (2014). Cloud: Herramientas para trabajar en la nube. (Páginas. 3 – 10). Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=5349776&ppg=8>
2. Contreras, S. J. G., & Navarro, G. M. A. (2015). Sistema de administración de contenidos de aprendizaje. (Páginas. 8 – 25). Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=5307940&ppg=32>
3. Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistema operativos. Recuperado de <https://ebookcentral-proquestcom.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228996&ppg=204>
4. Karzynski, M. (2014). Webmin Administrator's Cookbook. Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?URL=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=747086&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_1
5. Ministerio de educación y ciencia. Introducción a Linux. (Páginas. 1 - 40). Madrid. Recuperado de <http://www.mclibre.org/descargar/docs/manual-mec/mec-curso-ubuntu-606-200609.pdf>
6. Molina, R. F. J., & Polo, O. E. (2014). Servicios en red. Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3229687&ppg=104>
7. Muhammad Arifin, F., Andriana Mutiara, G., & Ismail, I. (2017). Implementation of Management and Network Security Using Endian UTM Firewall. Recuperado de <http://bibliotecavirtual.unad.edu.co/login?URL=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.C2217DDD&lang=es&site=eds-live&scope=site>
8. Muniz, J., & Lakhani, A. (2013). Web Penetration Testing with Kali Linux: A Practical Guide to Implementing Penetration Testing Strategies on Websites, Web Applications, and Standard Web Protocols with Kali Linux. Birmingham: Packt Publishing., Recuperado de http://bibliotecavirtual.unad.edu.co/login?URL=https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=644345&lang=es&site=ehost-live&ebv=EB&ppid=pp_7
9. Patawari, A. (2013). Getting Started with OwnCloud. (Páginas. 7 - 39). Birmingham: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?URL=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=620016&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_40
10. Shah, S., & Soyinka, W. (2007). Manual de administración de Linux. Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3191942&ppg=342>
11. Sanz, M. P. (2008). Seguridad en Linux: Guía práctica. Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3218549&ppg=68>
12. Singh, A. (2013). Instant Kali Linux. Birmingham [UK]: Packt Publishing. Recuperado de http://bibliotecavirtual.unad.edu.co/login?URL=https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=656227&lang=es&site=ehost-live&ebv=EB&ppid=pp_1
13. Torres, E. F., & Pizarro, G. A. M. (2017). Linux para usuarios. Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=4946218&ppg=76>
14. Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 121 – 148). Madrid, ES: IC Editorial. Recuperado de <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=4310544&ppg=126>